Disrupting In-Progress Network Intrusions by Algorithmically Forbidding the Excessive Writing of Duplicate-Hash Data Blocks within RAM

15 July 2023
Simon Edwards
Research Acceleration Initiative

Introduction

Six years having passed since the adoption of the practice of performing automated mutual system kernel hash verification to detect and sever compromised nodes from military networks in real-time, the full potential of data hashing has likely not yet been realized. Cryptographic hashes of data sets such as passwords have for decades been used to obviate the need for storing plaintext passwords (a security precaution that as of 2023, Facebook has somehow still failed to adopt,) but have become increasingly useful for confirming the integrity of the underlying code driving systems from the kernel level, upward, as well as other unexplored applications.

In high-security computing environments, the failure to keep multiple steps ahead of one's adversaries makes nearly inevitable the compromise of friendly networks. Security protocols must increasingly be implemented on an entirely automated basis in order to keep pace with automated attacks, but most importantly, should be both unique and unanticipated by the adversary. A good security protocol should not excessively disrupt the functionality of one's own network and should be simple enough that its implementation would neither drain system resources nor attract too much attention to its own existence.

Abstract

In a modern cyberattack in which the focus is on gaining undetected access to a system and subsequently exfiltrating sensitive data, an intruder must replace the proper system kernel with a modified kernel and this replacement must affect both the permanent copy of the kernel stored on the hard (or solid-state) drive, as well as the current state of the kernel within RAM. Overwriting the RAM "from page one" would result in system disruption that would likely be detected by existing intrusion detection algorithms.

In order to replace the legitimate kernel with a slightly modified, corrupt kernel, that corrupt kernel, which tends to be almost entirely identical to the original, must be written to a page somewhere in the unused portion of the RAM prior to the deletion of the original and ultimately, writing that corrupt kernel in the "proper" position starting at "page 1" of the RAM. Since the corrupted kernel must necessarily be largely identical to the original in order to remain system-compatible, there must necessarily, during the process of implementing such an attack, be a brief moment in which duplicate data is written in the system RAM in more than one place.

By forbidding the writing of excessive quantities of duplicate strings to RAM, these sorts of attacks may be halted before sensitive data is exfiltrated. While it is currently possible for a military network to "sever" a compromised node, a compromised node would still be free to exfiltrate any data stored on that network. Mutual kernel hash checking, while useful for protecting groups of networks, is not a panacea against all data theft. If, however, a kernel does not allow data (beyond a certain "density" of data strings) stored in RAM to be duplicated, it would be substantially more challenging for an intruder succeed in compromising sensitive data.

Obviously, it would not be practical to forbid all duplicate strings (the word "and" would be likely to appear many times, for instance) but it would be practical to halt systems in which an attempt is made to write large numbers of blocks of duplicated data which conforms to a particular profile. That profile would likely be defined as long strings that match the kernel with altered portions interspersed. Upon the heuristic detection of this sort of activity, a friendly network may be automatically halted to prevent the successful corruption of the system at large and inbound network traffic leading up to the suspicious event could be scrutinized retrospectively.

Conclusion

The implementation of such a protocol would substantially enhance existing security regimen and is deserving of further research.